IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF PENNSYLVANIA

CORNELIUS ALLISON, on behalf of himself and all others similarly situated,	:	CIVIL ACTION
v.	:	
AETNA, INC.	:	No. 09-2560

AMENDED ORDER

AND NOW, this 9th day of March 2010, upon consideration of Defendant's Motion to Dismiss the Amended Complaint (Doc. No. 14), Plaintiff's Memorandum of Law in Opposition thereto (Doc. No. 19), Defendant's Reply in support thereof (Doc. No. 22), and Plaintiff's Sur-Reply in further opposition thereto (Doc. No. 25), it is hereby ORDERED that Defendant's Motion is GRANTED. The Clerk of Court is directed to close this matter for statistical purposes.

I. FACTUAL AND PROCEDURAL BACKGROUND

Plaintiff Cornelius Allison seeks to bring a class action against Defendant Aetna, Inc. pursuant to the Class Action Fairness Act of 2005, 28 U.S.C. § 1332(d). (Am. Compl. ¶¶ 1, 3.) This case arises out of an alleged security breach of Defendant's online job application database. In January 2009, Plaintiff, who had previously worked for Defendant as an office assistant from December 1998 to May 2005, applied for a customer service position with Defendant using its website. (Id. at ¶¶ 37, 38.) He uploaded his personal information as well as his resume. (Id. at ¶ 38.) Defendant's website contained a "Web Privacy Statement," assuring users that it would not "sell, license, transmit or disclose this information" and touting the security measures that Defendant employed to protect such information against accidental or unauthorized access or disclosure. (Id. at ¶¶ 15-16.) In addition, Defendant also stated on the website that "[a]ll

information will be held in the strictest confidence." (Id. at ¶ 14.)

In May 2009, Defendant became aware of a breach of the job application website when applicants reported receiving spam ("phishing") emails purporting to be from Defendant. (Id. at ¶ 21.) The emails requested additional personal information in response to a job inquiry. (Id.) The job application website contained the email addresses of approximately 450,000 job applicants, the Social Security numbers of current and former employees, and the Social Security numbers, telephone numbers, addresses, and employment histories of individuals who had received job offers from Defendant. (Id. at ¶ 19.) In May 2009, "[Defendant] publicly announced that its job application website [had been] accessed by unauthorized persons." (Id. at ¶ 18.) Defendant stated, "We know for certain that emails were accessed, we don't know whether or not anything else was accessed." (Id. at ¶ 20.) Plaintiff does not allege that he received the phishing email, nor does he allege any other sort of misuse of the database information or his information specifically.

In addition to the public announcement, Defendant sent notification letters directly to Plaintiff and others potentially affected by the breach, including 65,000 current and former employees.[1] (Id. at ¶¶ 22, 39.) The letter stated that email addresses contained on Defendant's website had been accessed and that it was "possible that other personal information may have

[1] Plaintiff alleges that "[i]n May 2009, he received a letter from [Defendant] stating that his personal information *had been* accessed by an unauthorized person." (Am. Compl. ¶ 8 (emphasis added).) However, the letter from Defendant contains no such statement, rather the letter states that email addresses in Defendant's database were accessed, it is *possible* that other information was accessed, however Defendant was unable "to verify whether [Plaintiff's] personal information was accessed." (Aetna Letter to Plaintiff, attached to Am. Compl. as Ex. 1.)

been exposed." (Aetna Letter to Plaintiff, attached to Am. Compl. as Ex. 1.)[2] Defendant explained that it was unable to verify whether Plaintiff's information was accessed. (Id.) Defendant notified Plaintiff that the database contained his name, address, Social Security number, date of birth, phone number, email address, and employment history. (Id.) The website did not contain Plaintiff's banking, financial, or health information. (Id.) Defendant offered Plaintiff credit monitoring assistance and identity theft insurance. (Id.) It also encouraged Plaintiff to monitor his personal accounts and place a fraud alert on his credit file. (Id.)

Plaintiff alleges that Defendant failed to "adequately protect the private personal information of its current, former, and potential employees, including but not limited to their email addresses, names, Social Security numbers, home and/or office addresses, telephone numbers, employment histories, and other information ('Sensitive Information')." (Am. Compl. ¶ 3.) He claims that "as a result of [Defendant's] inadequate data security system, [Defendant's] website was hacked into by unknown third parties, and Class members' Sensitive Information was accessed and/or misused by unauthorized persons." (Id. at ¶ 5.) Plaintiff details the various ways in which Sensitive Information can be exploited, the dangers of identity theft, and the costs and inconvenience it causes its victims. (Id. at ¶¶ 10-13.) However, Plaintiff's only allegation of

---

[2] The letter attached to Plaintiff's Amended Complaint is a replacement letter he requested because he misplaced his original letter. (Am. Compl. ¶ 8.) In its Motion to Dismiss, Defendant provided a copy of the May 2009 form letter as well as a declaration verifying that the letter attached to Plaintiff's Amended Complaint is the same as the letter he received in May 2009. (See Def. Mot. Exs. A & 1.) When considering a motion to dismiss, the court may look to the allegations made in the complaint, the exhibits attached to the complaint, and any documents whose authenticity no party questions and whose contents are alleged in the complaint. Pryor v. Nat'l Coll. Athletic Ass'n, 288 F.3d 548, 560 (3d Cir. 2002). Documents attached to a defendant's Rule 12(b)(6) motion to dismiss may be considered if they are referred to in the plaintiff's complaint and if they are central to the plaintiff's claims. Id.

actual misuse relates solely to the phishing emails that were sent to others. (See id. at ¶ 21.)

Plaintiff describes the various remedial measures that he and other potential class members have been forced to undertake. (Id. at ¶¶ 24-29.) Specifically, Plaintiff has spent time reviewing bank statements, credit card bills, and credit reports; he has expended time signing up for credit monitoring; and he has suffered the inconvenience and delays attending fraud alerts. (Id. at ¶¶ 24-25, 40.) In addition to signing up for the services offered by Defendant, Plaintiff has also incurred out-of-pocket expenses for additional identity theft protection services. (Id. at ¶¶ 26, 41.) Plaintiff asserts that he and class members now "face a significant risk of identity theft" as evidenced by the phishing email as well as Defendant's own offer of credit monitoring and warning to individuals to take protective steps. (Id. at ¶ 28.) Finally, Plaintiff claims that he suffers anxiety, emotional distress, and loss of privacy. (Id. at ¶¶ 62, 70, 78, 86, 96.)

Plaintiff claims that Defendant is liable for negligence, breach of implied contract, breach of express contract, negligent misrepresentation, and invasion of privacy. Defendant moves to dismiss all claims pursuant to Federal Rules of Civil Procedure 12(b)(1) and 12(b)(6).

II. LEGAL STANDARD

Pursuant to Federal Rule of Civil Procedure 12(b)(1), a court must dismiss a matter if the court lacks subject matter jurisdiction. "The Constitution, Art. III, § 2, limits the federal judicial power to the resolution of 'cases and controversies.'" Interfaith Cmty. Org. v. Honeywell Int'l, Inc., 399 F.3d 248, 254 (3d Cir. 2005). "One element of the case-or-controversy requirement is that plaintiffs must establish that they have standing to sue." Id. "The Supreme Court has held that the 'irreducible constitutional minimum' of standing under Article III requires a plaintiff to establish three elements: an *injury in fact* . . . ; a *causal connection* between the injury and the

conduct complained of; and *substantial likelihood of remedy* - rather than mere speculation - that the requested relief will remedy the alleged injury in fact." Pa. Prison Soc'y v. Cortés, 508 F.3d 156, 160-61 (3d Cir. 2007) (citing Lujan v. Defenders of Wildlife, 504 U.S. 555 (1992)) (emphasis in original). "[E]ach element must be supported in the same way as any other matter on which plaintiff bears the burden of proof, i.e. with the manner and degree of evidence required at the successive stages of the litigation." Lujan, 504 U.S. at 561. "A 'federal court is powerless to create its own jurisdiction by embellishing otherwise deficient allegations of standing.'" Pa. Prison Soc'y, 508 F.3d at 161 (quoting Whitmore v. Arkansas, 495 U.S. 149, 155 (1990)).

When evaluating a motion to dismiss brought pursuant to Federal Rule of Civil Procedure 12(b)(6), "the facts alleged [in the complaint] must be taken as true and a complaint may not be dismissed merely because it appears unlikely that the plaintiff can prove those facts or will ultimately prevail on the merits." Phillips v. County of Allegheny, 515 F.3d 224, 231 (3d Cir. 2008). A court must draw all reasonable inferences in favor of the plaintiff. Id. However, "[f]actual allegations must be enough to raise a right to relief above the speculative level." Bell Atl. Corp. v. Twombly, 550 U.S. 544, 555 (2007). "To survive a motion to dismiss, a complaint must contain sufficient factual matter, accepted as true, to 'state a claim to relief that is plausible on its face.'" Ashcroft v. Iqbal, 129 S. Ct. 1937, 1949 (2009) (quoting Twombly, 550 U.S. at 570). "The plausibility standard 'asks for more than a sheer possibility that a defendant has acted unlawfully.'" Miles v. Twp. of Barnegat, 343 F. App'x 841, 844 (3d Cir. 2009) (quoting Iqbal, 129 S. Ct. at 1949). "A claim has facial plausibility when the plaintiff pleads factual content that allows the court to draw the reasonable inference that the defendant is liable for the misconduct alleged." Gelman v. State Farm Mut. Auto. Ins. Co., 583 F.3d 187, 190 (3d Cir. 2009) (quoting

Iqbal, 129 S. Ct. at 1949). "The assumption of truth does not apply . . . to legal conclusions couched as factual allegations or to '[t]hreadbare recitals of the elements of a cause of action, supported by mere conclusory statements.'" Miles, 343 F. App'x at 845 (quoting Iqbal, 129 S. Ct. at 1949).

III. DISCUSSION

Defendant argues that Plaintiff lacks standing because he has failed to allege an injury-in-fact. (Def. Mem. Law 13.) Defendant argues that "courts have recognized that allegations of 'increased risk of harm' and related costs for preventative measures are not legally cognizable injuries and have, therefore, dismissed the claims for lack of Article III standing." (Id.) Defendant focuses on the speculative nature of the harm to Plaintiff as well as the lack of imminency. (Id. at 4, 14.) Defendant contends, "The pleading describes only harm that might befall Plaintiff, sometime in the future, and only if Plaintiff's private data was in fact stolen by some unauthorized person and is some day used to commit identity fraud." (Id. at 4-5 (emphasis in original).) Defendant emphasizes that "the pleading does not allege that Plaintiff, or anyone else, has actually become the victim of identity theft as a result of the reported breach of the database." (Id. at 4.) Finally, Defendant argues that Plaintiff's alleged injuries resulting from the time and cost of credit monitoring "are not related to an actual injury, but to a potential injury in the indefinite future." (Id. at 14.)

Plaintiff contends that he has pleaded an injury-in-fact because he has alleged that he "suffered damages including out-of-pocket expenses, lost time, and an increased risk of identity theft." (Pl. Mem. Law 5.) Plaintiff argues that "[n]umerous courts in data breach cases have held that the theft of personal information is sufficient to confer standing, even without actual

identity theft. Standing in these cases is premised on out-of-pocket protective measures or the increased risk of identity theft." (Id. at 4.)

This case is part of a burgeoning area of law. As the district court in the Eastern District of Missouri recently explained,

> Database breaches appear to provide the basis for a new breed of lawsuits, and especially class action lawsuits, in which plaintiffs allege, as here, that the database handlers' negligence in developing and maintaining security measures have resulted in otherwise personal and confidential information being compromised, thereby increasing the risk of identity theft for those individuals whose information was so compromised. The remedies sought in these actions vary, but generally include costs for credit monitoring, costs for closing and opening financial accounts, and damages for emotional distress. Whether individuals have Article III standing to bring these lawsuits in federal court is a question that has been raised in many venues, to which divergent answers have been given.

Amburgy v. Express Scripts, Inc., --- F. Supp. 2d ----, No. 09-705, 2009 WL 4067218, at *1, 2 (E.D. Mo. Nov. 23, 2009). Until the Seventh Circuit's opinion in Pisciotta v. Old Nat'l Bancorp, 499 F.3d 629 (7th Cir. 2007), district courts consistently held that plaintiffs lacked standing to bring these claims.[3] In Pisciotta, plaintiffs alleged that "a third-party computer 'hacker' was able to obtain access to the confidential information of tens of thousands of ONB site users," however plaintiffs did not allege that anyone had been a victim of identity theft. 499 F.3d at 631-32. The

[3] See Randolph v. ING Life Ins. and Annuity Co., 486 F. Supp. 2d 1, 4, 7-8 (D.D.C. 2007) (plaintiff, who alleged that a laptop containing her personal information was stolen but did not allege any misuse, lacked standing under Article III); Bell v. Acxiom Corp., No. 06-0485, 2006 WL 2850042, at *1 (E.D. Ark. Oct. 3, 2006) (plaintiff, who alleged that a database containing her personal information was compromised and that information was illegally sold to a marketing company, lacked standing under Article III); Key v. DSW Inc., 454 F. Supp. 2d 684, 685-86, 690 (S.D. Ohio 2006) (plaintiff, who alleged that her information had been accessed by an unauthorized individual but did not allege misuse, lacked standing under Article III); Giordano v. Wachovia Sec., LLC, No. 06-476, 2006 WL 2177036, at *4-5 (D.N.J. July 31, 2006) (plaintiff, who claimed that defendant lost a hard copy of her personal information but did not allege that the information was stolen or in the possession of someone who might misuse it, lacked standing under Article III).

Seventh Circuit held that plaintiffs had standing, but dismissed the case for failure to state a claim pursuant to Federal Rule of Civil Procedure 12(b)(6). Id. at 634, 639-40. Since Pisciotta, courts in database breach cases have split on the issue of standing.[4] The Third Circuit has yet to address these types of cases. However, two district courts in New Jersey have considered whether a plaintiff, who alleges that his personal information was lost or compromised but alleges no misuse, has standing, and both courts found that the plaintiffs lacked standing to bring their claims. See Hinton v. Heartland Payment Sys., Inc., No. 09-594, 2006 WL 2177036, at *1 (D.N.J. Mar. 16, 2009); Giordano, 2006 WL 2177036, at *4-5. Proceeding once more unto the breach, this Court finds that Plaintiff in this particular case lacks standing to bring his cause of action.

An injury-in-fact "is an invasion of a legally protected interest that is (a) concrete and particularized, and (b) actual or imminent, not conjectural or hypothetical . . . ." Danvers Motor Co. v. Ford Motor Co., 432 F.3d 286, 290-91 (3d Cir. 2005). "Although 'imminence' is

[4] See Amburgy, 2009 WL 4067218, at *1, 5 (plaintiff, who alleged that unauthorized individuals accessed a database containing his personal information and threatened to publicize the personal information if the defendant did not pay them a certain amount of money, lacked standing under Article III); McLoughlin v. People's United Bank, Inc., No. 08-944, 2009 WL 2843269, at *1, 4 (D. Conn. Aug. 31, 2009) (plaintiff, who claimed that unencrypted back-up tapes containing her personal information were lost or stolen but did not allege misuse, had standing); Ruiz v. Gap. Inc., 622 F. Supp. 2d 908, 910, 912-13 (N.D. Cal. 2009) (plaintiff, who alleged that laptops containing his personal information were stolen but did not allege misuse, had standing); Hinton v. Heartland Payment Sys., Inc., No. 09-594, 2006 WL 2177036, at *1 (D.N.J. Mar. 16, 2009) (plaintiff, who claimed that his credit information was compromised in a electronic data breach but alleging no misuse, failed to allege an actual or imminent injury-in-fact); Caudle v. Towers, Perrin, Forster & Crosby, Inc., 580 F. Supp. 2d 273, 275, 280 (S.D.N.Y. 2008) (plaintiff, who alleged that laptop containing his personal information was stolen but did not allege misuse, had standing); Am. Fed'n of Gov't Employees v. Hawley, 543 F. Supp. 2d 44, 45-46, 50-51 (D.D.C. 2008) (plaintiff, who alleged that hard drive containing personal information was lost but did not allege misuse, had standing, although the holding was in part based on The Privacy Act of 1974).

concededly a somewhat elastic concept, it cannot be stretched beyond its purpose, which is to ensure that the alleged injury is not too speculative for Article III purposes - that the injury is 'certainly impending.'" Lujan, 504 U.S. at 564 n.2 (internal citations omitted). When sitting on the Third Circuit, Justice Alito noted that "[i]njury-in-fact is not Mount Everest." Danvers Motor Co., 432 F.3d at 294. "[A]n identifiable trifle is enough." Interfaith Cmty. Org., 399 F.3d at 254 (quoting United States v. Students Challenging Regulatory Agency Procedures (SCRAP), 412 U.S. 669, 689 n.14 (1973)). However, "pleadings must be something more than an ingenious academic exercise in the conceivable." SCRAP, 412 U.S. at 688.

Various circuit courts have recognized that an increased risk of harm can serve as the basis for an injury-in-fact. See Pisciotta, 499 F.3d at 634; Sutton v. St. Jude Med. S.C., Inc., 419 F.3d 568, 574-75 (6th Cir. 2005); Baur v. Veneman, 352 F.3d 625, 633-34 (2d Cir. 2003); Cent. Delta Water Agency v. United States, 306 F.3d 938, 950 (9th Cir. 2002); Friends of the Earth, Inc. v. Gaston Cooper Recycling Corp., 204 F.3d 149, 160 (4th Cir. 2000); see also Interfaith Cmty. Org., 399 F.3d at 257 (citing Gaston for the proposition that "[t]hreats or increased risk thus constitutes cognizable harm").[5] However, an increased risk of harm must still satisfy the

[5] Many of the courts that have considered increased risks of harm, including the majority of the cases relied on by the Seventh Circuit in Pisciotta, have done so in the context of potential environmental and/or medical/health harms. See, e.g., Pisciotta, 499 F.3d at 634 n.3. Courts have cautioned indiscriminately applying environmental and medical harm analyses to other sorts of injuries. In Key, the district court stated, "[T]he Court must acknowledge another important distinction between credit monitoring in the present case and medical monitoring. Medical monitoring necessarily involves preserving public health, a threat that does not present itself in the context of identity theft." 454 F. Supp. 2d at 691; see also Ruiz, 622 F. Supp. 2d at 914 ("[P]laintff has not presented any authority that endorses treating lost-data cases as analogous to medical monitoring cases. This Court doubts a California court would view these two types of cases as analogous."); Caudle, 580 F. Supp. 2d at 281 ("New York's interest in protecting the health of its citizens is stronger than in the protection of property."). As the Second Circuit recognized in Baur, "Because the evaluation of risk is qualitative, the probability

standing requirements of an injury-in-fact, set forth above. In Baur, the Second Circuit held that "an increased risk of contracting a food-borne illness from the consumption of downed livestock constitutes a cognizable injury-in-fact for Article III standing purposes." 352 F.3d at 631. However, the Second Circuit cautioned that "[g]iven the potentially expansive and nebulous nature of enhanced risk claims . . . [a plaintiff] must allege a 'credible threat of harm' to establish injury-in-fact based on exposure to enhanced risk." Id. at 637. The court explained,

> [L]ike all other aspects of standing, the injury-in-fact analysis is highly case-specific . . . and the risk of harm necessary to support standing cannot be defined according to a universal standard. Because the evaluation of risk is qualitative, the probability of harm which plaintiff must demonstrate in order to allege a cognizable injury-in-fact logically varies with the severity of the probable harm.

Id. (internal citations omitted); see also Massachusetts v. EPA, 549 U.S. 497, 526 n.23 (2007) ("The more drastic the injury that government action makes more likely, the lesser the increment in probability to establish standing." (quoting Mountain States Legal Found. v. Glickman, 92 F.3d 1228, 1234 (D.C. Cir. 1996))). In the context of an increased risk of identity theft, Judge Jerome Simandle held that "[t]he *mere possibility* of future harm fails to satisfy the standing requirements of the Supreme Court and Third Circuit of Appeals." Giordano, 2006 WL 2177036, at *4 (examining O'Shea v. Littleton, 414 U.S. 488 (1974), City of Los Angeles v. Lyons, 461 U.S. 95 (1983), and Luis v. Dennis, 751 F.2d 604 (3d Cir. 1984)) (emphasis added); see also Whitmore, 495 U.S. at 158 ("Allegations of possible future injury do not satisfy the

---

of harm which plaintiff must demonstrate in order to allege a cognizable injury-in-fact logically varies with the severity of the probable harm." 352 F.3d at 637. Because we find that Plaintiff alleges only a speculative harm under any standard, we need not define what, if any, type of increased risk of identity theft would suffice for purposes of Article III standing. However, we would caution that while environmental and medical harms are instructive, the harm resulting from identity theft is qualitatively different.

requirements of Art. III. A threatened injury must be 'certainly impending' to constitute injury in fact.").

Turning now to the facts of this case, we find that Plaintiff has failed to allege a sufficient injury-in-fact to satisfy the requirements of Article III.[6] Plaintiff's alleged injury of an increased risk of identity theft is far too speculative. First, Plaintiff's allegation that his personal information was even accessed is conjecture. Plaintiff never received the phishing email. In addition, Defendant's letter stated that they were unable to verify whether Plaintiff's information was even accessed. (See Am. Compl. Ex. 1.) Second, Plaintiff's own allegations suggest that the only information that the unauthorized individuals were able to access were the email addresses themselves. Plaintiff claims that "Class members face a significant risk of identity theft, evidenced by . . . [t]he hackers' efforts to extract personal information from Class members via sending phishing email messages. Hackers would not seek such information if they did not intend to misuse it." (Am. Compl. ¶ 28.) However, it would not be a reasonable inference for the Court to presume that hackers would seek such information, thereby risking exposure of their nefarious activities, if they had already obtained the same through unlawful means. Accordingly, even assuming that the hackers obtained Plaintiff's email address, it is highly speculative that they obtained any other information that would be necessary to commit identity theft. Similarly,

---

[6] This Court evaluates solely the standing of this particular Plaintiff and does not determine whether other individuals in the alleged class have standing to bring suit. It is well established that "in order to represent a class, [p]laintiffs must first be eligible to sue in their own right; 'what [they] may not achieve [themselves], [they] may not achieve as [] representative[s] of a class.' Therefore, named [p]laintiffs cannot meet standing requirements by relying solely upon the claims and potential standing of putative class members." Kahn v. Option One Mortgage Corp., No. 05-5268, 2006 WL 156943, at *7 (E.D. Pa. Jan. 18, 2006) (internal citations omitted).

Plaintiff does not allege that anyone else possibly obtained such information. Finally, Plaintiff is well aware of the previous phishing emails, so even assuming he received such an email now, the risk of him providing such information is slight. At best, Plaintiff has alleged a *mere possibility* of an increased risk of identity theft, which is insufficient for purposes of standing, and he certainly has not asserted a credible threat of identity theft.[7] Thus, Plaintiff lacks standing under any standard for increased risk of harm.

The decisions in Amburgy and Bell are instructive. In Amburgy, unauthorized individuals accessed a database containing personal information and threatened to expose such information if Defendant did not pay a certain amount of money. 2009 WL 4067218, at *1. The district court found that

> [f]or plaintiff to suffer the injury and harm he alleges, many 'if's' would have to come to pass. Assuming plaintiff's allegation of security breach to be true, plaintiff alleges that he would be injured 'if' his personal information was compromised, and 'if' such information was obtained by an unauthorized third party, and 'if' his identity was stolen as a result, and 'if' the use of his stolen identity caused him harm. These multiple 'if's' squarely place plaintiff's claimed injury in the realm of the hypothetical. If a party were allowed to assert such remote and speculative claims to obtain federal court jurisdiction, the Supreme Court's standing doctrine would be meaningless.

Id. at *5. Similarly, in Bell, an unauthorized individual obtained access to a database and then

---

[7] As Plaintiff has failed to establish an increased risk of identity theft, his claims for time and money spent on credit monitoring due to a perceived risk of harm cannot serve as the basis for an injury-in-fact. See Randolph, 486 F. Supp. 2d at 8 ("[A]n argument that the time and money spent monitoring a plaintiff's credit suffices to establish an injury 'overlook[s] the fact that their expenditure of time and money was not the result of any present injury, but rather the anticipation of future injury that has not materialized.'" (quoting Forbes v. Wells Fargo Bank, N.A., 420 F. Supp. 2d 1018, 1021 (D. Minn. 2006))); see also Am. Fed'n of Gov't Employees v. Styles, 123 F. App'x 51, 52-53 (3d Cir. 2004) ("[Plaintiffs'] preemptive action, while perhaps prudent, cannot be the basis for injury sufficient to satisfy Article III. To hold otherwise would allow the [plaintiffs] to manufacture its injury-in-fact and effectively eviscerate the Article III bar.") (internal citations omitted).

sold some of the information to a marketing company. 2006 WL 2850042, at *1. Plaintiff claimed that she was at an increased risk of identity theft and of receiving junk mail, even though she was not sure that her information was in fact stolen. Id. at 1-2. The district court dismissed plaintiff's complaint for lack of standing. Id. at 2. Plaintiff's allegations in this case are likewise too speculative to sustain standing under Article III.

Some courts have noted a "recent trend" towards finding standing following Pisciotta. See, e.g., McLoughlin, 2009 WL 2843269, at *4. As the Second Circuit noted in Baur, "the injury-in-fact analysis is highly case-specific." 352 F.3d at 637. This case is factually distinguishable from Pisciotta. Although the facts in Pisciotta are brief because the investigation was filed under seal, the Seventh Circuit explained that "the scope and manner of access suggests that the intrusion was sophisticated, intentional and malicious." 499 F.3d at 632. Plaintiff has not made factual allegations that would permit a similar inference of sophistication in this case. Rather, Plaintiff alleges that hackers obtained some email addresses which they then used in an attempt to elicit personal information via spam. (See Am. Compl. ¶ 28.) Plaintiff does not even allege that the hackers were successful in obtaining that additional information from anyone. Thus, in contrast to Pisciotta, Plaintiff has not alleged a credible threat of an increased risk of identity theft.

In Whitmore, the Supreme Court explained that "the requirement of an Art. III 'case or controversy' is not merely a traditional 'rule of practice,' but rather is imposed directly by the Constitution. It is not for this Court to employ untethered notions of what might be good public policy to expand our jurisdiction in an appealing case." 495 U.S. at 161. Plaintiff's alleged injury of an increased risk of identity theft is far too speculative based on the factual allegations

in this case. Therefore, Plaintiff lacks standing under Article III. Because Plaintiff lacks standing to bring this case, we need not address Defendant's Motion to Dismiss pursuant to Federal Rule of Civil Procedure 12(b)(6).

IV. CONCLUSION

For the reasons set forth above, it is hereby ORDERED that Defendants' Motion to Dismiss (Doc. No. 14) is GRANTED. The Clerk of Court is directed to close this matter for statistical purposes.

BY THE COURT:

/S/LEGROME D. DAVIS

Legrome D. Davis, J.